IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

| | |
|---|---|
| SRI INTERNATIONAL, INC., a California Corporation, | C. A. No. 04-1199 (SLR) |
| Plaintiff and Counterclaim-Defendant, | |
| v. | |
| INTERNET SECURITY SYSTEMS, INC., a Delaware corporation, INTERNET SECURITY SYSTEMS, INC., a Georgia corporation, and SYMANTEC CORPORATION, a Delaware corporation, | **PUBLIC VERSION** |
| Defendants and Counterclaim-Plaintiffs. | |

**SRI INTERNATIONAL, INC.'S REPLY IN SUPPORT OF ITS MOTION FOR
PARTIAL SUMMARY JUDGMENT OF NO ANTICIPATION BY THE
"EMERALD 1997" PUBLICATION**

Dated: July 10, 2006

FISH & RICHARDSON P.C.

John F. Horvath (#4557)
Kyle Wagner Compton (#4693)
919 N. Market St., Ste. 1100
P.O. Box 1114
Wilmington, DE 19889-1114
Telephone: (302) 652-5070
Facsimile: (302) 652-0607

Howard G. Pollack
Katherine D. Prescott
500 Arguello St., Ste. 500
Redwood City, CA 94063

Attorneys for Plaintiff and Counterclaim Defendant
SRI INTERNATIONAL, INC.

**TABLE OF CONTENTS**

## TABLE OF AUTHORITIES

**Page(s)**

## I.   INTRODUCTION

All the claims on which SRI moved for summary judgment require analysis of particular types of network traffic data. Defendants' original argument was based on the contention that disclosure of "application logs" and an implicit leap to "firewall logs" provided the alleged inherent disclosure. This was the basis of their own motion for summary judgment concerning EMERALD 1997[1]. While Defendants do continue to half-heartedly rely on their tenuous chain of unwarranted assumptions to argue that EMERALD 1997's disclosure of application logs necessarily discloses analysis of the claimed types of network traffic data, they still fail to identify any evidence that shows that application logs *necessarily*, as opposed to possibly, include the claimed types of network traffic data. As such, their position is incorrect as a matter of law.[2]

Faced with the weakness of their original theories of inherent anticipation, the Defendants create new ones, and now retreat from their experts' opinions regarding how EMERALD 1997 allegedly inherently anticipates the claims of the '615, '203, and '338 patents. They attempt to mask this retreat by referring to monitoring "data" from firewalls and mixing references to "logs" with "packets" in an effort to confuse the issues. In doing so they raise a completely new argument – that EMERALD 1997 allegedly suggests monitoring *packet data* (as opposed to logs) from a firewall.

These new theories are also without merit, ignore the requirements of the claims and lack any grounding in the disclosure of EMERALD 1997 or in the opinions of Defendants' five invalidity experts. Defendants argue with no support that EMERALD 1997 discloses using firewalls as a "data source for network packets" to be analyzed by

---

[1]   Defendants' Joint Motion for Summary Judgment of Invalidity Pursuant to 35 U.S.C. §§ 102 and 103. (D.I. 299).

[2]   Defendants apparently concede that disclosure of monitoring of SNMP traffic does not inherently disclose these types of data as they make no mention of this third, alternative argument in their opposition.

1

an intrusion detection system. [Opp. Br.[3] at 2]. They go on to argue that analyzing packets received from a firewall would inherently satisfy the Markush group. But nowhere does EMERALD 1997 make such a disclosure, nor do they cite to any support from their numerous experts for this conclusion. The only support for this new theory is conclusory attorney argument. Attorney argument is not evidence and cannot create a *genuine* issue of fact.

Defendants also raise arguments about alleged teaching of analyzing packets dropped or passed by a firewall. This argument, however, ignores the fact that the claims, as opposed to the specification, do not concern the analysis of dropped or passed packets. The claims require analysis of the particular types of network traffic data enumerated in the claims. Defendants' discussion of dropped and passed packets from a firewall is mere misdirection, irrelevant to the issue of whether EMERALD 1997 anticipates the claims.

Defendants' final "alternative," catch-all argument – that the mention of "datagrams" alone allegedly inherently discloses the claimed types of network traffic data – also must fail because it is likewise based only on attorney argument and bare conclusory statements from their experts.

## II.    SUMMARY JUDGMENT OF NO ANTICIPATION BY EMERALD 1997 IS APPROPRIATE

### A.    With respect to Defendants' prior theory, disclosure of analysis of application logs does not *necessarily* disclose analysis of the network traffic data of the Markush group.

The Defendants have given up on their argument that disclosure of SNMP traffic analysis itself inherently discloses analysis of the claimed categories of network traffic data. [Ex.[4] H at ¶ 253; Opening Br. at 9-10]. And they now bury, but do not entirely

---

[3]    Defendants' Opposition to SRI's Motion for Partial Summary Judgment of No Anticipation by the "EMERALD 1997" Publication ("Opp. Br.") (D.I. 342).

[4]    Unless otherwise noted all exhibits are attached to the Declaration of Kyle Wagner Compton in Support of SRI's Motion for Partial Summary Judgment of No

abandon, their contention that EMERALD 1997's disclosure of analyzing firewall logs inherently discloses analysis of the claimed categories of network traffic data. [Opp. Br at 7-8]. For the reasons discussed in both SRI's Opening Brief[5] and in its Response Brief[6], the mention of application logs in a list of possible sources from which an event stream may be derived [Ex. G at 356] is not the type of disclosure "which necessarily includes the subject matter embraced by the particular claim limitation" [Opp. Br. at 3] – the network traffic data of the Markush group – as the law requires. The discussion that follows focuses just on those points relating to the firewall log theory that defendants reiterate in their opposition brief.

Symantec's experts, Mr. Heberlein and Mr. Avolio, allege that EMERALD 1997's mention of possibly deriving an event stream from application logs necessarily discloses deriving an event stream from a firewall log where the firewall is necessarily capable of being configured to log packet data volume and network connection requests and denials and the firewall is necessarily so configured. [*See e.g.,* Ex. L at ¶¶ 13, 49, 50, 54, 59, 60, 62, 63, 66-68, 80; Ex. H at ¶ 252]. However, not all firewalls generate logs and certainly not all were capable of generating logs of the claimed types of network traffic. All the evidence identified by the Defendants to allegedly show otherwise actually only shows, at most, that some, but not all, firewalls could be configured to log certain data: "firewalls in 1997 *routinely* [not always] logged for review allowed packets or blocked packets" [Opp. Br. at 6-7)(emphasis added); *See also* Ex. L at ¶ 68]; "A *standard* [not every] firewall in 1997 also monitored and logged the amount of data send over each particular connection." [Opp. Br. at 7 (emphasis added); *see also,* Ex. L at

---

Anticipation by the "EMERALD 1997" Publication (hereinafter "Compton Decl."). (D.I. 278).

[5]  SRI's Opening Brief in Support of Its Motion for Partial Summary Judgment of No Anticipation by the "EMERALD 1997" Publication (hereinafter "Opening Br." or "Opening Brief") (D.I. 277).

[6]  SRI's Response to the Defendants' Joint Motion for Summary Judgment of Invalidity Pursuant to 35 U.S.C. §§ 102 & 103 ("Response Brief" or "Response Br.") (D.I. 339).

¶ 73]. In support of their position, the Defendants repeatedly point to the statement in "Building Internet Firewalls" which says "[m]ake sure the packet filtering router gives you the *option* of logging all of the packets it drops." [Brown Decl. at Ex. DD at 179[7] (emphasis added)]. Urging one to select a firewall with a logging *option* necessarily implies that there are firewalls without such capabilities. The Defendants also point to the statements that "you *could* use the firewall to log. . ." [Brown Decl. at Ex. AA at 639] and "you *could* configure them [firewalls] to record what they blocked." [Brown Decl. at Ex. V at 688-89]. Again this evidence only shows that it was possible for some firewalls to be configured to log certain information, not that firewalls all *necessarily* logged the claimed types of network traffic data at the relevant time, as required for inherent anticipation.

Even if a firewall had logging capability, it was not necessarily used at all, let alone used to monitor the claimed types of network traffic data. For example, Mr. Avolio highlights the SunScreen firewall and its logging capabilities [*see e.g.,* Ex. L at ¶¶ 37, 69, 70, 74],

<div align="center">**REDACTED**</div>

Also, "Building Internet Firewalls" explicitly suggests never logging certain types of information, for security reasons. [Brown Decl. at Ex. DD at 400]. As there is no evidence to support the Defendants' contention that disclosure of application logs necessarily discloses monitoring the types of network traffic required by the Markush group, summary judgment of no anticipation is appropriate.

**B.    With respect to Defendants' new theory, there is no evidence that EMERALD 1997 necessarily discloses analyzing packets received from a firewall.**

EMERALD 1997 discloses that "[u]nderlying the deployment of an EMERALD monitor is the selection of a target specific event stream. The event stream may be

---

[7]    Exhibit DD to Renee Dubord Brown's Declaration in Support of Defendants' Joint Motion for Summary Judgment Regarding Invalidity ("Brown Decl.") (D.I. 301).

derived from a variety of sources including audit data, network datagrams, SNMP traffic, application logs, and analysis results from other intrusion detection instrumentation." [Ex. G at 356]. Having abandoned their arguments based on the mere disclosure of SNMP traffic, and having recognized the weaknesses of their arguments based on audit data and applications logs, the Defendants progress through the disclosed list of possible data sources and now focus on "datagrams", which they equate with network packets. Specifically, rather than arguing, as before, that analysis of *logs generated by firewalls* necessarily discloses the types of network traffic data enumerated in the Markush groups, the Defendants allege for the first time that EMERALD 1997 allegedly teaches analysis of *packets* received from a firewall. The Defendants' switch from allegations based on the disclosure of "logs" from firewalls to allegations based on "packets" from firewalls is improper.[8] Regardless, there is no such disclosure in the reference.

Specifically, the Defendants claim that "EMERALD 1997 discloses the *use of firewalls as a data source for network packets*. The data provided by firewalls existing at the time necessarily included data corresponding to some of the recited categories in the claims" [Opp. Br. at 2 (emphasis added)] and that "EMERALD 1997 directly teaches monitoring network traffic at firewalls." [Opp. Br. at 4]. In support of their new argument, the Defendants highlight the disclosure in EMERALD 1997 that "[s]ervice monitors are dynamically deployed within a domain to provide localissed [sic] real-time analysis of infrastructure (*e.g.*, routers or gateways) . . . ." [Opp. Br. at 5; Ex. G at 355]. However, there is no mention of firewalls in this discussion. The Defendants realize this and thus attempt to import into the context of this statement the *sole* mention of a firewall in EMERALD 1997 appearing in another portion of the article altogether. Defendants provide no reason that one of skill in the art would have created this Frankenstein from what EMERALD 1997 actually discloses, and none is apparent. And even if the

---

[8]    Neither Defendants nor their experts previously raised this contention. Defendants should therefore be precluded from making this argument.

statements are combined in the way that Defendants suggest, the result they argue for does not follow. Neither statement mentions monitoring *packets* from a firewall, as opposed to "audit data," "SNMP traffic" or "application logs" – the last of which Defendants originally argued would be the implication to one of ordinary skill. Noticeably absent from the Defendants' new assertions regarding monitoring network packet traffic at or from firewalls are any citations to their numerous expert reports and declarations.  Thus, all the Defendants are left with is attorney argument that EMERALD 1997 contains the disclosure they wish were there.  Attorney argument, however, is not evidence.  *Invitrogen Corp. v. Clontech Labs., Inc.,* 429 F.3d 1052, 1068 (Fed. Cir. 2005) (establishing that "[u]nsubstantiated attorney argument regarding the meaning of technical evidence is no substitute for competent, substantiated expert testimony.  It does not, and cannot, support Clontech's burden on summary judgment.").  Thus there is no *genuine* issue of material fact that precludes summary judgment that EMERALD 1997 does not disclose the required types of network traffic data.

**C.    The Defendants' focus on packets dropped and passed by firewalls is misdirection.**

Whether EMERALD 1997 discloses analysis of packets dropped or passed by firewalls [Opp Br. at 5-6] is irrelevant to whether the claims of the patents-in-suit are anticipated.  The specification of the patents-in-suit discusses the generation of event streams from "discarded traffic (i.e., packets not allowed through the gateway because they violate filtering rules)" and "pass-through traffic (i.e., packets allowed into the internal network from external sources)." [Ex. A at 5:4-8].  EMERALD 1997 does not contain any comparable description. [Ex. B (Heberlein Report Ex. GG)].  Regardless, none of the *claims* of the '615, '203, or '338 patents, to which the prior art must be compared when analyzing anticipation, corresponds to these features of discarded or passed-through traffic described in the specification.  Even if EMERALD 1997 disclosed a monitor that focused only on discarded traffic, pass-through traffic, or packets to/from a

particular set of destination/source addresses as described in the specification [Ex. A at 5:4-8, 15-21] – and it does not – the *claims* still require that, from whatever subset of traffic one looks at (discarded, passed-through, or otherwise), the monitor base its measures or analysis on one of the specific types of network traffic enumerated in the Markush groups.

The Defendants do attempt to translate the monitoring of dropped packets to one of the enumerated types of traffic – network connection denials. Specifically, Defendants argue that "[p]ackets that a firewall did not allow into the network because they violated certain rules were, by definition, network connection denials." [Opp. Br. at 6]. This, again, is nothing but argument. The Defendants do not cite anywhere in the reports or declarations of their five expert witnesses on invalidity to support this statement because, not surprisingly, it is demonstrably wrong. Whether a firewall dropped a packet is not necessarily an indication of whether that packet was a network connection denial. A network connection denial is a type of packet. Firewalls drop packets for user-defined reasons that may or may not bear any relationship to the packet type, and in particular may drop packets for reasons unrelated to a network connection denial. "One of ordinary skill would understand that firewalls blocked packets based on rules. . ." [Ex. F ¶ 30]. Those rules or policies could be defined, for example, in terms of permitted or prohibited hosts. [Brown Decl. at Ex. AA at 638]. Thus, so long a packet was sent from a particular IP address, all packets would be dropped, regardless of the type of packet – network connection requests, network connection denials, data, data transfer errors, or any other type. Thus, just because a packet was blocked does not mean that it was a network connection denial.

Lacking support from their own experts, Defendants attempt to find support in quotes from the testimony of Dr. Kesidis and Mr. Porras. However, the cited testimony does not support the proposition urged. Dr. Kesidis did testify

[Brown Decl. at Ex. V at 688-

7

89]. He never testified with respect to the relationship between blocked packets and

network connection denials.                    **REDACTED**


Galvin Decl. (D.I. 343), Ex. A (Porras Tr.) at 376:22-377:11].


## REDACTED

[Galvin Decl., Ex. A at 378-79].

Thus the Defendants are left with a conclusory statement supported only by

attorney argument. "Attorney argument is no substitute for evidence," *Invitrogen,* 429

F.3d at 1068, and summary judgment is appropriate.

D. **Disclosure of datagram monitoring does not necessarily disclose analysis of the type of network traffic data required by the Markush group.**

The Defendants continue to maintain their "alternative" argument that the

disclosure of "datagrams[9]" as a source from which an event stream may be derived

necessarily discloses the specific types of data enumerated in the Markush groups. [Ex.

G at 356; Opp. Br. at 8, n. 17]. For the reasons discussed in SRI's Opening Brief, no

reasonable jury could conclude that the disclosure relating to datagrams in EMERALD

1997 inherently discloses the specific types of data required by the claims. [Opening Br.

---

9    Defendants also continue to characterize the categories of network traffic listed in the
     Markush group in a manner that renders the limitation meaningless. Defendants
     assert that "they [the categories of network traffic] broadly encompass most, if not all,
     network traffic." [Opp. Br. at 11].
     packet examined by the front-end '      **REDACTED**
                                                    [Compton Decl. at Ex. B (Kesidis
     Validity Report) at ¶ 26]. The testimony of the inventors is consistent.


**REDACTED**

8

at 10-12]. The Defendants' analogy of an intrusion detection system to a burglar alarm provides no support for their argument that the nature of the network attacks would have necessarily lead one of ordinary skill in the art to monitor one or more of the recited network traffic data categories. [Opp. Br. at 9]. Disclosure of a "burglar alarm to prevent entry into a house" does not necessarily require a specific type of monitoring – one could monitor doors, windows, motion, weight, temperature, or noise. As discussed in SRI's Opening Brief, many different techniques that are fundamentally different from the claimed inventions have been used to detect network attacks. [Opening Br. at 10-11].

The Defendants' attempts to use inventor testimony to support their datagram argument is also unavailing. The quotes that the Defendants highlight [Opp. Br. at 10-11] are irrelevant to question of what EMERALD 1997 teaches one of ordinary skill in the art.

**REDACTED**

Therefore, the cited testimony is irrelevant to whether the claimed types of traffic had been monitored in the context of the asserted claims and therefore whether EMERALD 1997 anticipates those claims.

### E.    The '212 patent is irrelevant to SRI's partial motion for summary judgment.

There are four patents-in-suit. [*See* Brown Decl. at Exs. A-D]. Three of these patents, the '615, '203, and '338, require analysis of particular categories of network traffic data. [*See* Brown Decl. at Exs. A-C]. SRI moves for partial summary judgment of no anticipation by EMERALD 1997 of these patents because EMERALD 1997 does not disclose the required categories of network traffic data. [*See generally*, Opening Br.]. The fourth patent, the '212 patent, does not contain this limitation. [*See* Brown Decl. at Ex. D]. EMERALD 1997 does not anticipate the '212 patent for other reasons, namely, EMERALD 1997 does not enable one of ordinary skill in the art to perform statistical analysis of network traffic on the scale of an enterprise network. [*See* Compton Decl., Ex. B (Kesidis Report re Validity) at ¶ 24; Response Br. at 14-17]. Enablement is an intensely factual inquiry. As detailed in SRI's Response Brief, genuine disputes of material fact remain that preclude summary judgment on this issue. For this reason, SRI did not move for summary judgment with respect to the '212 patent. Thus, contrary to the Defendants' assertions [Opp. Br. at 1], SRI did not concede anticipation of the '212 patent claims by its omission from SRI's Opening Brief.

## III.    CONCLUSION

For the foregoing reasons and those set forth in SRI's Opening Brief, SRI respectfully requests that the Court grant its motion for partial summary judgment of no anticipation by the EMERALD 1997 publication.

Dated:  July 10, 2006                    FISH & RICHARDSON P.C.


By:  */s/ John F. Horvath*
      John F. Horvath (#4557)
      Kyle Wagner Compton (#4693)
      919 N. Market St., Ste. 1100
      P.O. Box 1114
      Wilmington, DE 19889-1114
      Telephone:  (302) 652-5070
      Facsimile:  (302) 652-0607

      Howard G. Pollack
      Katherine D. Prescott
      500 Arguello St., Ste. 500
      Redwood City, CA 94063
      Telephone:  (650) 839-5070
      Facsimile:  (650) 839-5071

      Attorneys for Plaintiff/Counterclaim Defendant
      SRI INTERNATIONAL, INC.

## CERTIFICATE OF SERVICE

I hereby certify that on July 17, 2006, I electronically filed the foregoing document

with the Clerk of Court using CM/ECF which will send electronic notification of such

filing(s) to the following Delaware counsel.  In addition, the document will be served by

hand on Delaware counsel as follows:

| | |
|---|---|
| Richard L. Horwitz<br>Potter Anderson & Corroon LLP<br>Hercules Plaza<br>1313 North Market Street, 6th Floor<br>P.O. Box 951<br>Wilmington, DE  19899 | Attorneys for Defendant-<br>Counterclaimant<br>Internet Security Systems, Inc., a<br>Delaware corporation, and Internet<br>Security Systems, Inc., a Georgia<br>corporation |
| Richard K. Herrmann<br>Morris James Hitchens & Williams<br>PNC Bank Center<br>222 Delaware Avenue, 10th Floor<br>P.O. Box 2306<br>Wilmington, DE  19899-2306 | Attorneys for Defendant-<br>Counterclaimant<br>Symantec Corporation |

I hereby certify that on July 17, 2006, I have sent the foregoing document by

Federal Express overnight delivery to the following non-registered participants:

| | |
|---|---|
| Holmes J. Hawkins, III<br>Natasha Horne Moffitt<br>King & Spalding LLP<br>1180 Peachtree Street, NE<br>Atlanta, GA 30309 | Attorneys for Defendant-<br>Counterclaimant<br>Internet Security Systems, Inc., a<br>Delaware corporation, and Internet<br>Security Systems, Inc., a Georgia<br>corporation |
| Paul S. Grewal<br>Robert M. Galvin.<br>Lloyd R. Day, Jr.<br>Day Casebeer Madrid & Batchelder, LLP<br>20300 Stevens Creek Boulevard, Suite 400<br>Cupertino, CA  95014 | Attorneys for Defendant-<br>Counterclaimant<br>Symantec Corporation |

Theresa A. Moehlman
Bhavana Joneja
King & Spalding LLP
1185 Avenue of the Americas
New York, NY 10036

Defendant-Counterclaimant
Internet Security Systems, Inc., a
Delaware Corporation, and Internet
Security Systems, Inc., a Georgia
Corporation


/s/ *John F. Horvath*
John F. Horvath


80034097.doc